

A Deep Learning Based Social-aware D2D Peer Discovery Mechanism

Yu Long^{*}, Ryo Yamamoto^{**,††}, Taku Yamazaki^{†,††}, and Yoshiaki Tanaka^{*,††,‡}

^{*}Department of Computer Science and Communications Engineering, Waseda University

^{**}Graduate School of Informatics and Engineering, The University of Electro-Communications

[†]Department of Electronic Information Systems, Shibaura Institute of Technology

^{††}Global Information and Telecommunication Institute, Waseda University

[‡]Department of Communications and Computer Engineering, Waseda University

long_yu@akane.waseda.jp, ryo-yamamoto@uec.ac.jp, taku@shibaura-it.ac.jp, ytanaka@waseda.jp

Abstract— With the demand for rapid exchanges of information, device to device (D2D) communications become one of the essential components of next-generation network architecture. To realize efficient D2D communication, peer discovery plays an important role since the discovery result strongly affects further performance. Most of the researches on peer discovery in D2D communication are based on discovering proximity devices to recognize nearby destination devices. In particular, some researches focus on time slot distribution to broadcast address information for discovering proximity devices. Moreover, other researches pay attention to user grouping with different beacon probing signals. However, these peer discovery mechanisms do not consider the risks that source devices may encounter malicious devices in real situations. As a solution to this, this paper proposes a peer discovery mechanism which applies the social network relationship information to exclude malicious devices. The proposed mechanism contributes to decrease the probability of encountering malicious devices and enhances the efficiency of peer discovery by excluding malicious devices. Simulations clarify that the base station (BS) extracts trusted candidates among devices to quantify the trust degree of devices based on the potential social information.

Keywords— D2D communication, peer discovery, malicious device, social network information, deep neural network

I. INTRODUCTION

In the evolution of 5G-based wireless communication technology, the performance of such as technology continues to improve the efficiency from the perspective of network capacity, spectrum utilization, and so forth. On the other hand, from the viewpoint of users, rich communication services and the user demands require higher data switching rates and more connections to ensure lower cost, higher security, and stable communication. Device to device (D2D) communication, that is one of the essential technologies of 5G, potentially ameliorates the performance of the communication system and expands the prospects of cellular communication applications. When devices of users exist in proximity, the devices can directly transmit data to each other through the D2D communication, and therefore D2D communication guarantees

them to reuse the cellular network resources under the control of base station (BS) [1]. Therefore, some researches that the cellular network promotes and assists D2D communication have been proposed to improve spectrum utilization [2], [3].

In D2D communication, peer discovery, mode selection, resource allocation and interference management [4] are the main components. Here, this paper focuses on peer discovery since it is the essential procedure to determine communication pairs among peer candidates and peer selection affects the efficiency of D2D communication.

In the peer discovery process, user devices require to recognize the presence of potential candidate devices firstly and there are two types of discovery approaches in traditional schemes. The first one is the centralized approach that the pair selection is done from the network-side and performs paging or other signalling to mediate discovery process by recognizing D2D candidate devices and potential services in a centralized manner. In addition, this approach improves the network resource utilization since it can coordinate time and frequency of D2D communication from the network-side. However, this approach suffers from the difficulties in stability and scalability due to the irregular behaviours derived from individual device control by users. The second one is the decentralized approach that the devices exchange control signals from each other to discover themselves in a distributed manner. If users are placed inside their device communication range, they can recognize idle devices with each other whenever they require without coordination with others. Therefore, the decentralized discovery is realized only by exploiting the ad-hoc communication in practical situations. However, there remains an important issue that the decentralized ad-hoc approach has high energy consumption [1]. In addition, this approach may be difficult to find suitable candidates since devices can only perform randomized beacon without coordination or any other information.

Recently, a novel approach that utilizes social network information to discover peers have been studied [1] [5]. Social networks have penetrated people's daily life and the networks also have played an important role in our daily life. The rapid

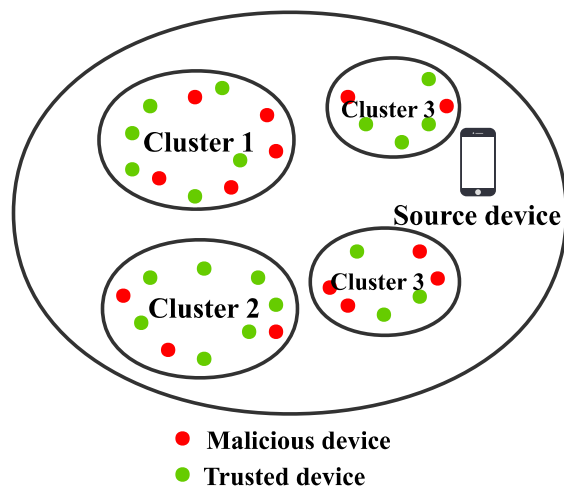


Figure 1. Cluster division model. Each cluster includes trusted devices and malicious devices.

development of social networks is not only for the dissemination of information, but also an important way for users to show their own value and their interests, and to maintain the interpersonal relationship. Consequently, it is important to understand the characteristics and behaviours of users in the social networks to analyse the content characteristics and information dissemination effect in social networks. The social network is a system that provides communication service to users, which is closely related to social relationships between users. Previous studies of social network knowledge usage have emphasized potential advantages in peer discovery [1] [5]. By utilizing the social domain information, we can tackle the challenging issue of trusted D2D communication pair detection more effectively.

This paper proposes an ad-hoc peer discovery mechanism based on social network information. The proposed mechanism can obtain trusted devices based on social network information to exclude malicious devices using a deep neural network (DNN) model. To combine peer discovery with potential social network relationship, the proposed mechanism realizes to find out potentially malicious devices. As a result, it can remove malicious devices and increase the probability to recognize trusted devices in a long-term situation such as a school or a company.

II. RELATED WORKS

Previous works devote much effort to superior mechanisms. In [7]-[9], these mechanisms consider the target selection based on distance and energy consumption. Each user's device broadcasts its' own address information at a specific time slot designed previously. The mechanism helps to reduce the communication cost from the view of the individual user. However, the mechanism forces each device to consume huge network resource by the notifications. Paper [11] provides a discovery scheme based on location information of each device. Devices in a cellular network are distributed with unequal proximity beacon according to the location valuation such as duration, switching rate, and transmission speed. However,

their approach only focuses on the performance improvement of devices and networks only by using the information such as throughput, energy and Signal- Noise Ratio (SNR) from the viewpoint of the network. In a practical situation, each device can obtain more valuable information such as user's preference and connection frequency associated with each user since each device belongs to each user. Therefore, it is important to utilize the users' social information and interactions to control the network.

As an application of social information in D2D communication, some advanced works have been studied [1] [5]. Paper [5] provided a social-aware peer discovery technique in cellular networks to improve discovery efficiency. In this technique, devices are classified into different clusters based on social interaction frequency. Source devices recognize the destination devices according to their demand directly from different clusters with smaller target devices range in the peer discovery. Paper [5] probed the scheme based on social attributes and service attributes [1]. It quantifies the trust degree between user pairs, and it serves them as the basis of neighbour discovery combined with users' social attribute requirements. However, there still remains an ongoing challenge due to potentially malicious devices since they don't consider the impact of potentially malicious devices on worthless connections. Potentially malicious devices also propagate spams and take up resources to a certain extent.

It is worthwhile mentioning that real dynamic gets stuck with potentially malicious devices, which is not considered in previous research. In [3] [5], devices are divided into several clusters according to their social metrics, such as communication frequency and duration. Each cluster is distributed with optimal beacons probing rate with constant intervals, which means that each cluster takes up an unequal time slot to broadcast their address information per cycle. In Figure 1, the dimension of the cluster indicates the probability of being recognized in peer discovery. More proportion of possession signifies higher probability. Under the circumstance, the source device requires to recognize the cluster firstly. Then, reliable devices are detected from the set of devices in the cluster. Therefore, the probability can be described as the following Eq. (1).

$$P_f = P_{\text{cluster}} \times P_{\text{trust}} \quad (1)$$

where P_f is the final probability of trusted devices being recognized, P_{cluster} is the probability of the cluster being recognized, P_{trust} is the probability of trusted devices being recognized in the cluster.

In real environments, source devices tend to recognize the destination devices randomly without using extra information. In other words, there is the possibility that source devices cause meaningless connections for the existence of malicious devices. Devices may result in consuming their energy since the recognition process might last for several loops.

The proposed mechanism is based on our previous research [6] and has a similar work flow. Prior works only focused on the part of using deep learning in extracting potentially malicious devices. It achieved separating trusted devices and malicious devices combining with social network information.

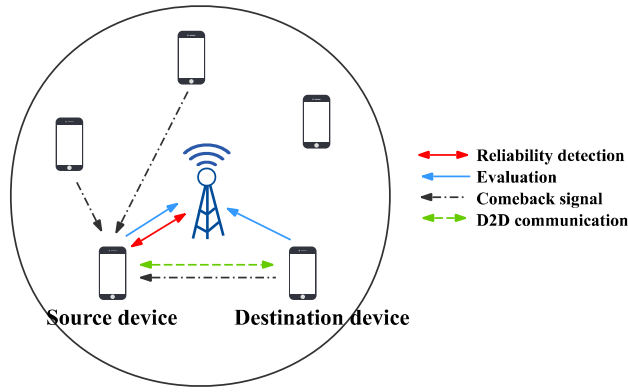


Figure 2. Process of the proposed model.

However, previous research didn't mention the whole process of peer discovery.

III. SOCIAL-AWARE PEER DISCOVERY MECHANISM

In this paper, we advance the detail peer discovery process model combining with social network information, which reveals the superiority in connection success rate comparing to other works. Furthermore, users' evaluation is also considered to update the individual's social information. In a long-term relation environment such as a school or a company, we can conjecture the trust degree of devices from the social network information. In general, it is considered that trusted users are always feasible to serve positive information in frequent interaction with others, which makes communication more efficient. Therefore, it is also considered that there is a significant correlation between device communication efficiency and trust degree. For example, user devices prefer to communicate with familiar devices. Hence, it is also considered that social information can be employed in a prior detection system.

To recognize trusted devices and exclude malicious devices, this paper proposes a peer discovery mechanism using a recognition of trusted devices based on a deep neural network (DNN) model. As different from the aforementioned works, we consider that the BS executes detection tasks of trusted devices using a deep neural network (DNN) model in the proposed mechanism. The objective of the mechanism is to minimize the number of candidate devices, which filters out malicious devices according to the trust degree of users.

A. System Model

This section defines a system model for the proposed mechanism. We adopt the common social scenario in [5] as the followings: Trust degree among individuals could be reflected by social interaction with others and established along with the formed partnership such as friendship and colleague. Replicating the true dynamic, the communication horizon of the cellular network is assumed as R . For a simplified consideration, border communication is neglected in the paper.

TABLE I
NOTATIONS IN THE PROPOSED SYSTEM MODEL

Symbol	Definition
n	The number of devices detected by the source device
B_{idle}	Idle device set
B_t	Idle device set with their credit information
f_i	Connection frequency to device i
h_i	Connection success rate to device i
l_i	Contact duration to device i
F	Connection frequency set
H	Connection success rate set
L	Contact duration set
M	Trust degree set
C_i	Trust degree to device i

Algorithm 1: Proposed Trusted Devices Detection Algorithm

- 1: The source device broadcasts a signal and sets a timer.
- 2: Idle devices reply an ACK to the source device.
- 3: The source device makes an idle device set B_{idle} and sends B_{idle} to BS.
- 4: **for** i **in** B_{idle}
- 5: BS searches f_i, h_i, l_i of user i
- 6: BS forms f_i, h_i, l_i into sets F, H, L respectively
- 7: **end for**
- 8: BS puts F, H , and L into the neural network
- 9: BS gets a set M and makes a set B_t
- 10: BS sends B_t to the source device

The sequence of the proposed detection mechanism is described below and as shown in Figure 2.

To reflect the effect of social interactions among users to peer discovery, the proposed mechanism uses three types of social network information: (1) connection frequency, (2) connection success rate, and (3) contact duration. Firstly, connection frequency has been proposed in [1], [5] as the key factor to show the communication enthusiasm of devices. In addition to the factor, connection success rate and contact duration have been used. However, in real environments, it is assumed that malicious devices may appear in general. The malicious devices often broadcast spams and end up the communication for causing Distributed Denial of Service (DDoS) due to the network congestions. Therefore, the use of connection success rate and contact duration may get rid of these malicious devices. The details of them are described in III-C. To collect the social network information, each device stores and updates social network information when occurring social interactions. Then, each device transmits an evaluation of the social network information in a perspective of the device to BS to collect and aggregate the social network information among local devices.

When a user wants to use D2D communication, the user's device, a source device, broadcasts its identification information to detect local devices as peer candidates. On receiving the message, devices reply an acknowledgment (ACK) to the source device if it is in an idle status. After that, the source device forms an idle device set $B_{idle} = \{1, 2, \dots, n\}$

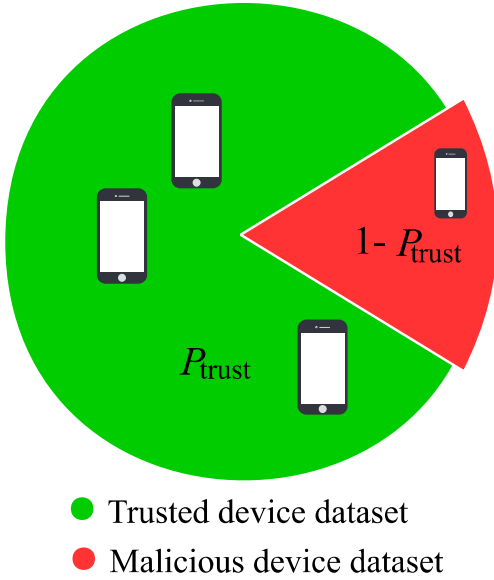


Figure 3. Process of the proposed model. Trusted devices and malicious devices are separated via the proposed mechanism.

to seek the trust degree of these devices. Here, n means the number of idle devices detected by the source device based on the ACK reception.

Then, the source device sends B_{idle} to the BS for excluding potentially malicious devices using DNN. Here, the proposed mechanism concentrates the all detection tasks of trusted devices and malicious devices to the BS to reduce the computational load of users' device. Note that the features for calculating trust degree of each device are described in III-C and the detailed algorithm of DNN is described in III-D.

B. Trusted Peer Discovery Process based on DNN

This section describes the trusted peer discovery process of the proposed model cooperate with the associated BS as shown in Figure 3. In the proposed mechanism, all devices are classified into two device types, trusted devices and malicious devices, to distinguish them correctly as candidates for peer discovery. Combining the detection tasks with social network information, BS uses a deep neural network (DNN) to distinguish the devices. By introducing DNN, the network will be able to adaptively filter out malicious devices. The detailed trusted device detection algorithm is shown in Algorithm 1 with the summarized notation in Table 1.

In the detection system, we employ three different metrics from social network features for decision as inputs into DNN. The potential social features are collected by the BS in advance via the information uploading of devices [11] and then analysis of DNN model is settled in the BS. The DNN model regards the three social network features as inputs to estimate trust degree of devices. The proposed neural network consists of three layers. It is assumed that the proposed mechanism runs in long-term relation environments such as schools or companies since people frequently build and keep the social relationship in these environments. Hence, users in familiar circumstances can establish their relationship via frequent interactions. Therefore, it is considered that the potential social

information is contributed to the BS in the paper. In the proposed mechanism, P_f is described as below.

$$P_f = P_{DNN} \quad (2)$$

Where P_{DNN} is the probability of trusted devices being recognized after evaluating the devices by the proposed peer discovery process based on DNN. Through DNN processing, trusted devices can be extracted out directly.

C. Social Network Information

In the detection task, we adopt the following information based on social activities: (1) connection frequency, (2) connection success rate, and (3) peer contact duration.

(1) Connection Frequency: The connection frequency means that a device is recognized by other devices for peer discovery [1], [5]. Positive devices are more active in transmission for reciprocity. They can obtain useful information while sharing information at the same time. The BS manages a set F to show the frequency of each device, $F = \{f_1, f_2, \dots, f_i, \dots, f_n\}$ where f_i represents the mean number of connections to a device i in a period as calculated by Eq. (3).

$$f_i = \frac{1}{n-1} \sum_{j=1}^n u_{ij}, i \neq j \quad (3)$$

where u_{ij} is the connection frequency of user i detected by device j , respectively.

(2) Connection Success Rate: The connection success rate represents a rate for successful connection with other devices. Here, we define a set $H = \{h_1, h_2, \dots, h_i, \dots, h_n\}$ where h_i represents the accumulated success rate of all connection of a device i in D2D communication as calculated by Eq. (4).

$$h_i = \sum_{j=1}^n a_{ij} + \sum_{j=1}^n b_{ij}, i \neq j \quad (4)$$

where a_{ij} is the success rate of the peer connection from device i to device j , b_{ij} is the success rate of the peer connection from device j to device i respectively. Malicious devices perform worthless actions to waste resources. To improve connection efficiency, we should enhance successful connection rate to lessen worthless actions. This part consists of the process of recognizing destination devices and being recognized as destination devices.

(3) Contact Duration: Mean contact duration represents the duration of each communication. Usually, an effective transmission sustains for enough long period [4], and it generally requires more time to share useful information. There is a kind of harmful influence that malicious devices execute short-time connections to transmit spams which results in a congestion. Therefore, we define a set $L = \{l_1, l_2, \dots, l_i, \dots, l_n\}$ where l_i represents an accumulated contact duration of device i .

$$l_i = \sum_{j=1}^n t_{ij}, i \neq j \quad (5)$$

$$t_{ij} = \frac{1}{P_{ij}} \sum_{k=1}^{P_{ij}} |t_{s,ijk} - t_{e,ijk}| \quad (6)$$

where t_{ij} is the mean contact duration between device i and device j , P_{ij} is the times of connections between node i and node j , $t_{s,ijk}$ and $t_{e,ijk}$ are the start and end of D2D communication of a k -th time between node i and node j .

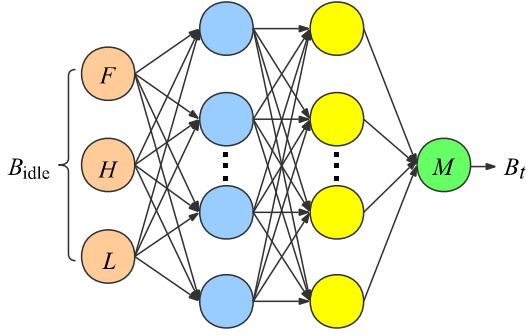


Figure 4. Framework of the detection system.

D. DNN Model for Recognizing Trusted Devices

Deep neural network (DNN), which consists of multi-layer neural networks, is generally interpreted in terms of the universal approximation theorem or probabilistic inference. The proposed system uses the DNN model to make the connection between the trust degree and social information via neural networks. Devices in D2D communication include hidden social network information. In the view of previous researches on people's social behaviours, the trust degree of devices can be estimated via social interaction information. The proposed DNN model constructs a structure with 2 fully connected layers. In addition, each layer consists of 10 neurons. Here, we obtain the social credit set of the source device $M = \{c_1, c_2, \dots, c_i, \dots, c_n\}$ where $c_j \in \{0, 1\}$ as an output of the DNN algorithm. Note that the symbol c_i means the device i is a trusted device or a malicious device.

After the detection of trusted devices and malicious devices, The BS forms a new set $B_t = \{1: c_1, 2: c_2, \dots, n: c_n\}$ and returns the set to the source device. To use the information of B_t , the source device can choose trusted devices based on social credit values and it starts D2D communication based on the information. The process of the detection system is concluded in Figure 4.

After D2D communication, pairs of devices make an evaluation of this communication and send it to the BS including the features described above. The evaluation is used to update devices' social information described above and it may increase or decrease the trust degree of devices. Therefore, to contribute accumulating the credit of devices, it improves the detection accuracy of trusted devices and malicious devices.

IV. PERFORMANCE EVALUATION

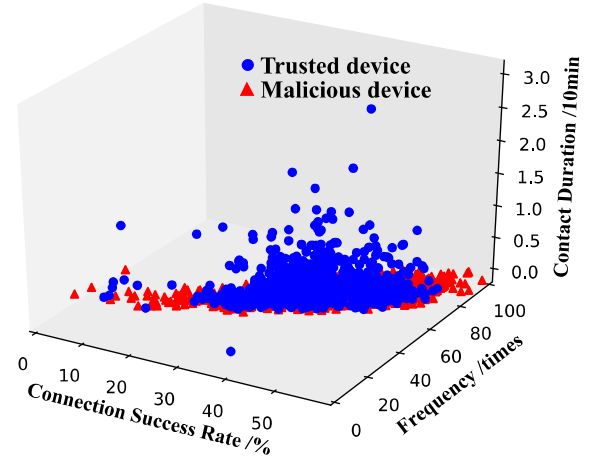
In this section, we carry out extensive simulations to evaluate the performance of our purposed deep learning based peer discovery mechanism with social relationship information. The settings and compared simulation results are presented as follows.

A. Simulation Environments and Settings

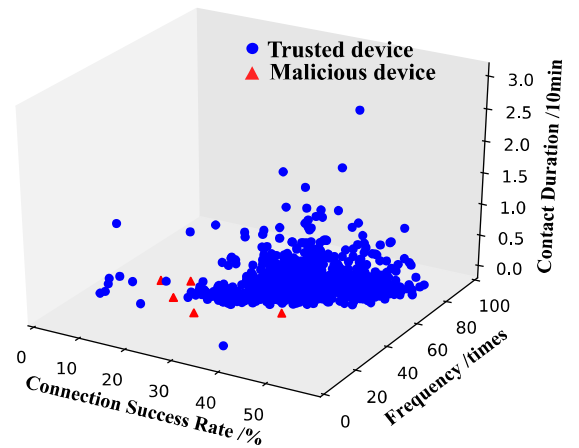
We use two simulations to evaluate our proposed mechanism.

(1) **Simulation 1** uses device distribution to test the performance. In the process, we use an existing dataset [11] which collects the interaction information among students in a school to reproduce realistic environments. Each device contains detailed communication factors, including connection frequency and connection success rate, as well as contact duration to each user. Individuals are appointed with trust degree to be trusted or malicious. Therefore, two device datasets are established with and without the proposed mechanisms.

(2) In **simulation 2**, in order to deeply investigate the merits in connection success rate, we compare the proposed mechanism with existing works [3][4]. In comparison, we assume peer discovery as an issue of trusted device recognition. Here, two presumptions are settled: (1) Potentially malicious devices exist. (2) The cluster with the highest trust degree is always chosen.



(a) Original device distribution.



(b) New device distribution.

Figure 5. Device distribution.

B. Results Analysis

Simulation 1

(1) We compare device distributions of the original one without removing malicious devices and evaluate the fundamental performance of the proposed mechanism as shown in Figure 5. For the comparison, we train the detection system with the existing dataset. As a result, the accuracy of the system attends a high level in extracting trusted devices at about 95% after the training.

Figure 5 (a) shows the original device distribution in a natural environment based on the dataset. In the figure, trusted user devices and malicious user devices are mixed together. The aim of the proposed mechanism is to separate them with the DNN model.

Figure 5 (b) shows the new device distribution with the proposed mechanism. The result shows that the proposed system can remove most of the malicious devices correctly. Then, the source device can acquire a set of trusted devices from the BS in the peer discovery. Hence, it becomes a higher probability to make a meaningful connection with the candidate devices by the proposed peer discovery mechanism since the source device can avoid connecting with potentially malicious devices.

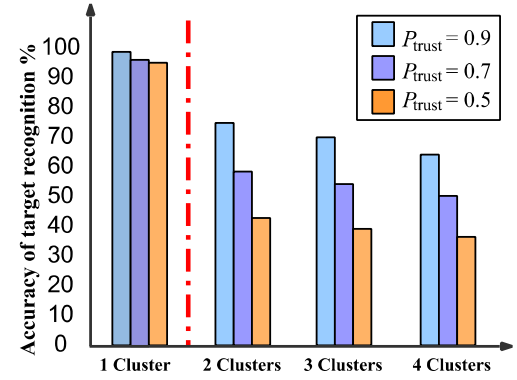
Simulation 2

(2) In the process of existing works, each cluster is independent. Therefore, the source device can only recognize the target from one cluster per cycle. In practice, devices in all clusters are possible to be assigned as the candidate device. For a simplified consideration, we employ the circumstance that the source device always recognizes the target from the cluster with the highest trust degree. In other words, we just choose the cluster with the largest probability each time. At the same time, P_{trust} keeps the same in each cluster.

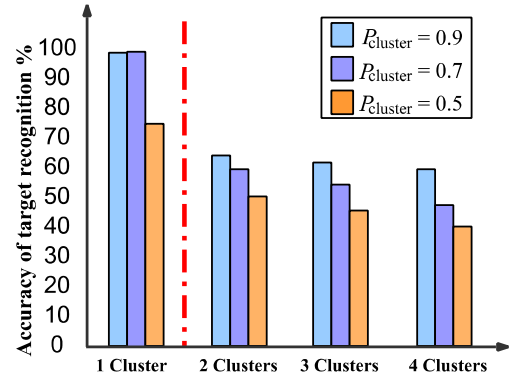
Figure 6 illustrates the performance of trusted devices' recognition under two occasions. On the left part of the red line, the proposed mechanism is adopted. All devices focus on one cluster. In the right part, previous works are conducted. Devices are divided into different clusters according to their trust degree.

Figure 6 (a) shows the result of the accuracy of target recognition when varying P_{trust} and fixed $P_{\text{cluster}} = 0.8$. Figure 6 (b) shows the result of the accuracy of target recognition when varying P_{cluster} and fixed $P_{\text{trust}} = 0.7$ where P_{trust} is the percentage of non-malicious devices and P_{cluster} is the percentage of being-recognized probability of the cluster.

The result shows that the proposed mechanism achieves higher performance than the existing work. The proposed mechanism can extract trusted devices from whole peer candidates by using DNN model. Hence, it is a key process that provides the peer selection with a scheme on reducing meaningless-connection targets. On the other hand, the existing work cannot remove the malicious device sufficiently since it mainly pays attention into community division with common interests. Therefore, the peer discovery of the existing work still suffers from the existence of malicious targets. As a



(a) Accuracy of the trusted device recognition with different P_{trust} with $P_{\text{cluster}} = 0.8$.



(b) Accuracy of the trusted device recognition with different P_{cluster} with $P_{\text{trust}} = 0.7$.

Figure 6. Performance of detecting trusted devices.

result, the fact causes extra resource consumptions on meaningless connections. Derive from this, we follow with interest in filtering out malicious users in advance. The proposed mechanism can emerge as an interesting peer candidate for peer discovery.

V. CONCLUSION

This paper proposed a D2D peer discovery mechanism underlying cellular networks based on social network information. The proposed mechanism could recognize trusted devices and malicious devices by using DNN model with social network relationship. In addition, a BS employs the index to recognize trusted devices and it recommends them to the source devices for constructing worth connection.

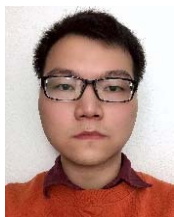
In the course of this analysis, we have demonstrated that the method realizes the trusted candidate detection via potential social relationship information. In the simulation results, the proposed mechanism realizes that the source device avoids malicious devices.

As a future work, the motivation of users is supposed to be considered in the research. The instability of connection influences the communication channel and Signal-to-Noise Ratio (SNR). Therefore, future research will pay attention to the

combination of social network information and physical network information.

REFERENCES

- [1] Z. Zhang, L. Wang, D. Liu, and Y. Zhang, "Peer discovery for D2D communications based on social attribute and service attribute", *J. Net. Comput. Appl.*, vol. 86, no. 7, pp. 82-91, May 2017.
- [2] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, and Turányi, "Design aspects of network assisted device-to-device communications," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 170-177, March 2012.
- [3] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communication in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96-104, Jun. 2012.
- [4] D. Wang and X. Wang, "An interference management scheme for Device-to-Device multicast in spectrum sharing hybrid network," *2013 IEEE 24th Annual Int. Conf. Symp. Personal, Indoor, and Mobile Radio Communications (PIMRC 2013)*, London, UK, Sept. 2013.
- [5] B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, "Social-aware peer discovery for D2D communications underlying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2426-2439, May 2015.
- [6] Y. Long, R. Yamamoto, T. Yamazaki, and Y. Tanaka, "Device to Device Peer Discovery Mechanism Based on Social Network Information", *2018 IEICE Communications Society Conference*, No.BS-7-12, pp.S-47-S-48, September 2018.
- [7] X. Lin, J. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3DPP device-to device proximity services," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 40-48, April 2014.
- [8] F. Baccelli, N. Khude, R. Laroia, J. Li, T. Richardson, S. Shakkottai, S. Tavildar, and X. Wu, "On the design of device-to-device autonomous discovery," *2012 4th Int. Conf. Commun. Syst. Netw. (COMSNETS 2012)*, Bangalore, India, Jan. 2012.
- [9] K. Doppler, C. B. Ribeiro, and J. Knecht, "Advances in D2D communications: Energy efficient service and device discovery radio," *2011 2nd Int. Conf. Wireless Commun. Veh. Tech. Inf. Theory and Aerospace & Electron. Syst. Tech. (Wireless VITAE 2011)*, Chennai, India, Feb. 2011.
- [10] W. Lee, J. Kim, and S. W. Choi, "New D2D peer discovery scheme based on spatial correlation of wireless channel," *IEEE Trans. Veh. Tech.*, vol. 65, no. 12, pp. 10120-10125, Dec. 2016.
- [11] Kaggle, "The dataset for simulation," <https://www.kaggle.com/hikarilu/socail-network-in-schools>, accessed on Jan. 2018.



Yu Long received the B.S. degree in communication and information engineering from University of Electronic Science and Technology of China, Chengdu, China, in 2017. He is currently working toward the M.S. degree with the Department of Computer Science and Communications Engineering, Waseda University, Tokyo, Japan. His current research interests include device-to-device communications, social network, deep learning. He is a member of IEICE.



Ryo YAMAMOTO received his B.E. and M.E. degree in electronic information systems from Shibaura Institute of Technology, Tokyo, Japan, in 2007 and 2009. He received D.S. in global telecommunication studies from Waseda University, Tokyo, Japan, in 2013. He was a research associate at Graduate School of Global Information and Telecommunication Studies, Waseda University, from 2010 to 2014, and has been engaged in research in wireless communication networks. He is presently an assistant professor at Graduate School of Informatics and Engineering, The University of Electro-Communications. He received the IEICE young researcher's award in 2010, the IEICE Network System Research Award in 2014, the CANDAR/ASON Best Paper Award in 2014, IEICE Communications Society Distinguished Contributions Award in 2017, IEICE Information and Communication Management Distinguished Contributions Award in 2014 and 2017. His current research interests are ad hoc networks, sensor networks, IoT/M2M networks, and network protocols for the networks. He is a member of IEICE and IEEE.



Taku Yamazaki received the B.E. and M.S. degrees in electronic information systems from Shibaura Institute of Technology, Tokyo, Japan, in 2012 and 2014, respectively. He received D.E. in computer science and communications engineering from Waseda University, Tokyo, Japan, in 2017. He was a research associate at Department of Communications and Computer Engineering, Waseda University, from 2015 to 2018. He is presently an assistant professor at Department of Electronic Information Systems, Shibaura Institute of Technology. He is also presently an adjunct researcher at Global Information and Telecommunication Institute, Waseda University. He received IEICE Network Systems Research Award in 2014, the CANDAR/ASON Best Paper Award in 2014, IEICE Young Researcher's Award in 2015, IEICE Network Software Best Poster Award in 2016, and IEICE Network Systems Young Researcher's Encouragement Award in 2018. He is a member of IEEE, IEICE, JSEE.



Yoshiaki Tanaka received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo, Japan, in 1974, 1976, and 1979, respectively. He became a staff at Department of Electrical Engineering, the University of Tokyo, in 1979, and has been engaged in teaching and researching in the fields of telecommunication networks, switching systems, and network security. He is presently a professor at Department of Communications and Computer Engineering, Waseda University. He received the IEICE Best Paper Award, the IEICE Achievement Award, the IEICE Distinguished Achievement and Contributions Award, the Okawa Publication Prize, the Commendation by Minister for Internal Affairs and Communications, etc. He is an honorary member of IEICE.